SFG | SHARED ASSESSMENTS

Building Best Practices
Briefing Paper

C-Suite Call to Action
Risk Management Through A Different Lens

Executive Summary

Setting the Tone for 2021: Out of the Shifting Landscape, Opportunity Arises

While the key elements of robust Tone at the Top haven't changed – those remain Management, Culture, Structure, and Communications - industry is recalibrating how those elements are incorporated into effective and efficient Third Party Risk Management (TPRM) governance. There is good reason to recalibrate.

This Call to Action suggests what organizations should be doing based on recent events – including the pandemic and the unprecedented scale of recent environmental disruption. Learnings from this period of upheaval are well worth examining in depth in C-suites and board rooms. This paper identifies some of the issues that can be solved today, as well as others that may not be remediable now but deserve examination once TPRM programs are better positioned to mitigate specific risks in the future.

The level of disruption being experienced across sectors offers organizations the opportunity to change the tone around risk management from one where risk management is deemed a necessary but unwelcome cost to one of collaboration in which the integration of risk management strategy and business strategy, benefiting all stakeholders.

We can rebuild our collective resilience by examining where we can be proactive in our messaging about risk – across our own organizations, as well as in interactions with our third parties, their suppliers, and our customers.

Mismanagement is becoming a watchword due to a cascade of breakdowns in systems, including governance structures. At the same time that industry groups are pushing back against regulators substantial impacts from mismanagement are being seen across industries:

BPI Endorses Legislative Compromise to Reform Anti-Money Laundering Framework and End Anonymous Shell Companies. Bank Policy Institute. "This compromise is the culmination of years of bipartisan work and signals to the world that the U.S. will no longer provide a safe haven for human traffickers, terrorists and other illicit global actors."

Boeing Board Accused in Lawsuit of Lax Oversight During 737 MAX Crisis The Wall Street Journal. "Two influential proxy advisers recommended shareholders vote against key board members to protest the handling of the 737 MAX debacle."

USAA ordered to improve risk management, information security. American Banker. The bank agreed to pay a $3.5 million fine and $12 million in restitution to 66,000 customers.

JPMorgan fined $250 million for problems in advisory business . American Banker. the company "will pay a $250 million fine for poor risk management practices and conflicts of interest in its advisory business."

Regulators Fine Citigroup $400 Million Over 'Serious Ongoing Deficiencies.' The Wall Street Journal. Fed, OCC order the nation's third-largest bank to fix its risk-management systems.

The message being conveyed is that norms must change. We need to do things differently than we've done them before. This Call to Action provides some perspective on what and how we can move the needle in risk management, particularly third party risk management.

Our Call to Action – Collective Solution Building

The Call is to imbed risk considerations into organizational process. This allows for risk-based planning and more effective implementation, enabling superior outcomes over time while better protecting the enterprise. Determine what your organization's C-suite can do to convey the message that risk belongs at the table imbedded into any planning process – from the board level down – right from the start and not as an afterthought.

The Need to Pivot around Emerging Risks

Risk professionals need to collectively determine – along with C-Suite and board input – how to develop a proactive stance in uncharted circumstances. Shifting from reactive to proactive will require a clear understanding of:

- how well equipped a company is to deal with potential risks;
- how these risks may affect the company's third and Nth party population; and
- ultimately the impact on service or product delivery.

Traditional approaches that rely solely on point-in-time assessments can no longer keep up with rapidly changing or emerging risks. Facilitating an agile response requires leveraging indicators that allow for better forecasting to guide oversight and monitoring as close to real-time as possible.

Risk governance components that require examination during a re-assessment of a company's position span Management, Culture, Structure, and Communications. *Note: These components are strategic in nature and changes to them should be supported by the top of an organization in order to succeed.*

TONE AT THE TOP	There is a need to ensure that senior risk personnel have appropriate stature within an organization.[i] Stature indicates that executive level risk officers (chief risk officer, chief audit officer, etc.) are well respected, have clearly defined CEO and board supported authority in their areas, and are included in executive committee level management meetings.
TRAINING	There is a growing and well-recognized need for qualified professionals to enhance the understanding of the value of risk prediction for board members, analysts, and risk managers.
SUPPLY CHAIN DISRUPTION	Supply chain disruption demands a clear understanding of the complexity of supply networks in the face of a relatively unstable global environment. Assess, evaluate, and learn what is working and what is obstructive in order to help and enhance business resilience plans. Companies have to devise feasible scenario testing at the most radical comprehensive levels and build from the knowledge gained from these exercises. Before disruption occurs, map the networks, plan for alternate providers/suppliers, and develop and test scenarios.
RISK METRICS AND COMMUNICATIONS	There is a need for appropriate cross-category, quantitative metrics that allow management to see deeper into the supply chain, as well as a need for speed in assessing the horizon (i.e., forecasting). The results should be made available to guide decision making across the enterprise, as needed.
COMPLIANCE AND OTHER REGULATORY ISSUES	There is a need to anticipate organizational needs in the face of changing regulatory guidelines and to make incremental improvements in resourcing to meet those emerging requirements. Issues must be communicated in order to challenge business units to anticipate the need for compliance, and to adopt commendable cohesive, existing and emerging best practices.
SERVICE LOCATION RISKS	There is a need to better understand and manage critical risks related to location to ensure a comprehensive risk and resiliency program.

Viewing Risk Through A Different Lens

A lens in which risk considerations are imbedded into organizational process, including in planning, provides the opportunity for efficient strategic goal setting and conducting and evaluating business operations that result in significantly improved outcomes. Determine how to make your program work comprehensively and with dexterity within the organization's mission, goals, and responsibilities.

Key Areas to Consider	Strategic Value	Action Points
IDENTIFY AND CLOSE GAPS IN TPRM MATURITY	Agility is directly tied to preparation – for the existing environment and for the risk challenges that are still to come. The opportunity exists to reassess and revise approaches and actions according to findings, so that greater agility and risk management effectiveness can be developed.	Ascertain which processes can be adjusted to be more nimble. Determine what risk areas are not currently examined and should be reviewed.
EXAMINE THIRD PARTY PORTFOLIOS	Examine and document emerging third and Nth party risks that might affect your organization. Determine where concentrations risks might disrupt operations.	Determine what you need to do operationally to adjust to those new risks. Document those policies and processes.
CREATE ACCOUNTABILITY THROUGH A DEDICATED RISK RADAR	Accountability has to be maintained for monitoring and analyzing risks, and then creating and executing appropriate action plans. This requires visibility and transparency to ensure risks are being examined across the depth and breadth of what may impact your organization.	There must be a process within your governance structure that is constantly analyzing risk. This process requires all stakeholders to be at the table.
RISK MUST BE CONTEXTUALIZED	Rigid processes discourage and eliminate critical thinking around what is relevant to your circumstances, lines of business, and the evolving landscape in which you operate. Continuous quality improvement (CQI) for programs requires the ability to re-observe and orient quickly in a changing landscape to foster effective decision making.	*Note: This is an iterative activity, which employs a feedback/feed forward loop to contextualize observations around risk needs to be native to your processes.* The OODA Loop – which employs an Observe, Orient, Decide [heuristics], Act – is a proven method that meets this need.
TIE TPRM GOVERNANCE INTO YOUR ORGANIZATION'S ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK	Many organizations have a waterfall perception on regulatory change, particularly those in the financial and health care sectors. Be aware that changes mandated through ballot initiatives do not typically provide the same long lead times as emerging legislation does for adapting and advocating for the impact those rules may have on business models.	Build inter-company and peer relationships to support better responses to changes in regulation and risk.
BE AWARE OF RED FLAGS, WHICH CHANGE OVER TIME	Market dynamics and credit risk are examples of key financial indicators that are used predictively.	Evaluate what red flags you have marked as triggers for risk and enhance your risk management processes to allow those indicators to come to the attention of appropriates risk leaders and executives without delay – NOW.
EARLY RISK IDENTIFICATION EMPOWERS BUSINESS GROWTH	Governance and control is about how to best accomplish risk management, not about simply stopping processes from occurring that are necessary for business operations. Instead, engage in risk management discussions at the start, involving risk management during procurement processes.	Imbed risk considerations into organizational processes, including early in system design lifecycles. Meet with senior leaders of business units to drive the concept of risk-based design and analysis that can be achieved a with minimal amount of disruption. As new products and processes are just being kicked off, risk managers need to ask: "What do you see as a hurdle that we should be addressing right now?"

Key Areas to Consider	Strategic Value	Action Points
DEVELOP BETTER PLANNING AND EXERCISE GROUP DYNAMICS	It is imperative that processes allow for a quick pivot when needed. Learn from what hasn't worked, not just from successes, and pass that learning along! Better collaborative planning naturally sets the stage for improved results.	Make this a regular part of program work ahead of any catastrophes, in small, focused groups and across departments. Conducting multi-day scenario planning exercises help get people together in a deliberate way with common risk thinking.
INTERACT WITH PEERS TO LEARN WHAT IS POSSIBLE, FEASIBLE, DOABLE, AND SURVIVABLE	Shared Assessments provides a cross-vertical analysis of due diligence that allows organizations to look across a broad spectrum of companies and learn from the impacts those organizations have felt. Those impacts can help portfolioand other risk managers gain perspective on what agile strategies look like and how those can be applied to your organization.	Armed with a best practice based, peer guide understanding, more realistic scenarios can be exercised run and more secure supply chains can be developed.

Strive to incorporate agility into existing processes and platforms enterprise-wide. Be sure to communicate the message that Risk Management will do whatever is needed to help business units execute effectively, including resolving issues around perceived conflicts with existing infrastructure, systems, and processes. Document obstacles and determine how to best adapt to the risk environment. To better accommodate the inevitable changes to the risk environment, the team may be able to alter product/service lines, mitigate the risks, or accept the risks.

The Risk Horizon – Areas to Contemplate for 2021

- **Emerging Technologies:** Work needs to continue on developing and injecting strategies and tactics for anticipating emerging risks which may not already be on the risk radar. Lapses in this area currently are not anticipating a risk and therefore not preparing; and – most egregious – seeing a risk and not acting.
- **Regulatory Shifts:** Environmental, Social, and Governance (ESG) is coming to the forefront in regulation. ESG risks include modern slavery, supply chain risks, conflicts of interests between companies and Nth parties parties that may remain under the radar while you scale your program. It is incumbent on companies to align their ability to identify conflicts of interest and determine what management and oversight is needed within third party relationships to align with regulation. Privacy is also at the forefront, both domestically in the US and abroad.
- **Geopolitical and Geographical Risks:** The complexity of this landscape continues to grow, with unprecedented natural disasters, pandemic-related shutdowns of human resources and infrastructure, geopolitical, and economic instability.
- **Increase Risk Program Budgets to Decrease Risk:** While program scalability is critical, senior leaders must take into account that the risk landscape for third parties is ever growing and more complex, meaning that programs need to be sufficiently funded to be able to perform all the necessary oversight that regulators, clients, and customers demand.

Conclusion – Seeing through a Different Lens

It is imperative to fundamentally effect organizational change. Key steps to imbedding risk considerations in all activities to hone a better understanding of emerging risks and enhancing risk management processes – and organizational processes generally – include:

1. Go through the exercise of examining what potential new risks – including cascading risks – your industry may face and how that may impact your need to monitor for those risks. This exercise will provide the C-suite with a better understanding of blinds spots where better management and oversight may prove valuable. Ask your managers what they are they hearing in the industry is emerging concerns around supply chain and third party/nth party risks.

2. Work to apply verifiable metrics and arithmetic analysis around the potential impacts of unknowns, and be prepared for those impacts by having flexibility in your program's framework and company's risk model.

3. Refresh organizational risk appetite frameworks to align with emerging risks.

4. Perform these steps in an iterative process that supports and encourages brainstorming and effective problem solving.

In this way, you can see the world through the multiple lenses that the complexity of the global environment encompasses.

Risk management should be perceived as a value added process. To help reinforce value, learn to speak in the terms of your audience.

	**REPORTS AND PRESENTATIONS** have to clearly explain the value proposition that risk management provides. Use cases can demonstrate how processes get bogged down because risk management was brought in too late in the lifecycle.
	**TALK WITH PEOPLE** at all levels of the organization to make sure your processes are "Fit for Purpose." When they are not, find ways to improve process with input from all stakeholders.
	**ACT AS PARTNER** – Do it globally, to break any perception that risk managers are doomsday messengers. It may be obvious why involving procurement may be an efficient activity; however, it can be less obvious what value risk management can bring to the organization over time.
	**EXAMINE YOUR PROGRAM.** Is your third party risk program funded for the technology needed to drive meaningful reporting, risk indicators and scalability in an ever changing ecosystem? Can the existing framework be nimble and pivot quickly when major events occur and risk impact changes? Are risk assessments going beyond reactive point-in-time calendar reviews and instead taking into account emerging regulatory needs, environmental changes, and technology advancements?

To support your efforts, conduct fact-based decision making. Wherever possible demonstrate quantitatively, as qualitative evaluations often lack the impact analysis required for effective decision making. Determine what you can do to clarify operational, reputational, and other types of risks that are hard to measure? Take the time to demonstrate what risks can disrupt key value points (e.g., cost savings, innovation, better improved customer service, etc.). And demonstrate the value that your supply chain brings to the organization and what risks and impacts can affect this value.

You'll find the results worth the effort.

Additional Resources

- Shared Assessments Program TPRM Framework
- Shared Assessments Vendor Risk Management Maturity Model (VRMMM)
- Institute of Risk Management Horizon Scanning: A Practitioner's Guide
- KPMG Third party risk management: Thriving in the new reality
- McKinsey & Company: Meeting the future: Dynamic risk management for uncertain times
- Selected Shared Assessments White Papers:
  - Documenting Your TPRM Program Business Case
  - Building Best Practices in Third Party Risk Management: Involving Procurement
  - Fourth Party Risk Management: Supply Chain Issues and Emerging Best Practices
  - Innovations in Third Party Continuous Monitoring: With a Name Like OODA, How Hard Can It Be?

Acknowledgments

This briefing paper is the effort of the Shared Assessments Program's U.S. Steering Committee members. All of Shared Assessments Program activities are conducted under the direction and oversight of Shared Assessments Steering Committees. To learn more about our member-driven committees and working groups, please contact us at: (505) 466-6434 or info@ sharedassessments.org.

About Shared Assessments

The Shared Assessments Program is the trusted leader in Third Party Risk Management, with resources to effectively manage the critical components of the Third Party Risk Management lifecycle. Program resources are creating efficiencies and lowering costs for all assessment participants; kept current with regulations, industry standards and guidelines and the current threat environment; and adopted globally across a broad range of industries both by service providers and their outsourcers.

Shared Assessments offers opportunities for members to work alongside peers to address global risk management challenges through committees, awareness groups, interest groups, and special projects. For more information on Shared Assessments, please visit: http://www.sharedassessments.org.

Shared Assessments committees and working groups create deliverables such as this briefing paper as part of a larger body of agnostic research, articles, educational and certification materials, and other resources that support best practice development in third party risk management.

The Shared Assessments Program TPRM Framework encompasses the full body of work from these ongoing efforts. As a dynamic, living document, the Framework informs our educational materials, program tools, and other resources, which are regularly modified and updated to reflect new risks, the changing regulatory and industry environments, and the continuing evolution of effective risk management approaches. The Framework is available to members at: https://sharedassessments.org/framework/

Disclosure: The content of this series is not intended to convey or constitute legal advice, is not to be acted on as such, and is not a substitute for obtaining legal advice from a qualified attorney. These materials include the strategic and tactical processes deemed the most generally applicable to and useful for the most parties, both outsourcers and third parties. This material is not intended to be inclusive of every case required by statute or regulation for any specific industry, nor those mandated by any and all industry standards.

Endnotes

i Stature is defined as "the ability and authority to influence decisions and effect change throughout the organization, procure resources necessary to carry out responsibilities, escalate issues as needed to senior management and the board, and observe or participate on relevant management committees." Federal Reserve System Notice. Section 43. January 11, 2018. https://www.federalregister.gov/documents/2018/01/11/2018-00294/proposed-supervisory-guidance